REMARKS/ARGUMENTS

Favorable consideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-20 are pending in the application, with Claims 1, 15, 16 and 19 amended by the present amendment.

In the outstanding Office Action, Claim 15 was objected; Claims 1-20 were rejected under 35 U.S.C. § 102(e) as being anticipated by Clark (U.S. Patent No. 5,982,897).

Claim 15 is amended to overcome the outstanding objection. Claims 1, 15, 16 and 19 are amended to conform with MPEP claim drafting guidelines. No new matter is added.

Briefly recapitulating, Claim 1 is directed to a method for satellite positioning using positioning signals which are sent out by the various satellites of a satellite constellation under the control of a set of ground stations from which said satellites receive control signals. The position signals are available to be picked up by individual user receivers. The method includes a) emitting, from the set of ground stations, periodically renewed direct transformation functions which are addressed respectively to each satellite of said satellite constellation and applying the direct transformation function received by each satellite to encode the positioning signals emitted therefrom.

The method further includes, upon each request from a user receiver addressed to a user servicing station, verifying that the user receiver has a right to a privileged-user status and, in the event that the verification is positive, addressing to the user receiver reverse transformation functions that are inverse to the direct transformation functions applied at the satellites from which it receives positioning signals. The reverse transformation functions constitute an interpretation key for interpreting the positioning signals by applying the reverse transformation functions for decoding them.

Clark describes a system and method for GPS key distribution and use.[1] In particular, Clark describes discloses a method and system wherein satellites that are visible from a hostile area do not transmit a decryption key for a high-precision navigational data, while satellites that are only visible from non-hostile areas do.[2] Hence, all the users situated in a "non-hostile" area benefit from an unrestricted access to high-precision navigational data. However, contrary to the Official Action, Clark does not disclose or suggest Applicants' claimed feature of "emitting, from said set of ground stations, periodically renewed direct transformation functions which are addressed respectively to each satellite of said satellite constellation and applying the direct transformation function received by each satellite to encode the positioning signals emitted therefrom."

Furthermore, the designation of a "non-hostile" area is not completely reliable. Therefore, there is a need to prevent potentially hostile users from accessing high-precision navigational data, whatever their location. One embodiment of Clark provides a partial solution to this problem. Clark discloses a method wherein satellites broadcast an encoded decryption key.[3] Authorized users receive a registration key, which allows them to decode the decryption key, and then use the latter to decode the high-precision navigational data. In this embodiment there is indeed a registration procedure, and a key is distributed to registered users. However, this key does not correspond to the decryption key recited in Applicants' Claims 1, 15 and 19.

Claims 1, 15 and 19 clearly state that the "user servicing station" (and not the satellites) transmits to the registered user (and does not broadcast) the actual decryption key. For further security, as recited in Claim 4, the decryption key can be coded, and the registered user uses the registration key to decode the decryption key. On the contrary, in Clark the

[1] Clark, abstract.
[2] Clark, column 4, lines 33 – 65.
[3] Clark, column 6, lines 44 to 63.

"user servicing station" issues a registration key, and the satellites themselves broadcast the coded decryption key. Clark neither discloses nor suggests any ability for already registered users to actively request the specific delivery of the actual decryption key (in either an unencoded or coded form) from a user servicing station, which has full power to refuse the delivery even if the user holds a valid registration code.

Furthermore, in Clark, the period of use of the registration key needs to have a much longer period of use than the encryption key.[4] Therefore, once the registration key has been distributed, the system manager has no possibility of preventing the registered user from accessing the high-precision navigational data, even if it begins acting in an unauthorized way. For example, if the user is a civil airplane which receives, before taking-off, a registration key which is valid during all the scheduled flight time, if the airplane exits the authorized flight path, it will still benefit from the high-precision navigational data and the only way to prevent that would be to perform an unscheduled change of the code used for encoding the decryption key. This would affect all the registered users, by making their registration keys useless.

However, in Applicants' claimed invention, the registered user has to ask for the decryption key(s) each time he needs to access to the high-precision navigational data (the registered user cannot rely on a previously obtained decryption key, because the encryption key could have changed since then). At each request, the identity and behavior of the user can be checked, and the registered user can be easily declared non-privileged even if it owns a regular registration key. No passage in Clark either discloses or suggests such a system and method, wherein a decryption key ("reverse transformation functions") is selectively transmitted upon request, to authorized users only, by a user servicing station.

[4] Clark, column 6, lines 44 to 46.

Clark does not disclose nor suggest transmitting, together with such a request, a copy of the latest positioning signal received by the user receiver as recited in Claims 2, 8, 9, 10, 13 and 14. Instead, Clark discloses

- a method wherein all the satellites transmit encrypted data and a decryption key, which is accessible to all users, which transmit neither a request, nor positional data;[5]
- a method an apparatus wherein a decryption key is broadcast in encoded form and wherein all registered users can autonomously decode said decryption key and use it to accede to high-precision navigational data;[6]
- a drawback of his invention, namely the fact that even users outside an "hostile" area can suffer from an intermittent denial to accede to high-precision navigational data;[7]
- the usé of a beam-steering technique;[8]
- the possibility of providing privileged users with the master key used for generating the encryption key, so that privileged users benefit from an unlimited access to high-precision navigational data;[9] and
- a periodical broadcasting of the decryption key to all users outside a "hostile" area.[10]

Therefore Claims 2, 8, 9, 10, 13 and 14 are novel and non-obvious in view of Clark.

Clark also does not disclose nor suggest supplying an identifier to the user and broadcasting it to various servicing stations to which the user is likely to address a request calling for a decryption key as recited in Claims 3 and 4. Instead, Clark discloses:

- the use of ground transmitters to broadcast a decryption key, without the need for any request, in regions near an hostile area;[11] and

[5] Clark, column 3, line 50 to column 4, line 10.
[6] Clark, column 7, lines 1 to 33; column 7, line 50 to column 8, line 5.
[7] Clark, column 5, lines 16 to 26.
[8] Clark, column 5, lines 45 – 56.
[9] Clark, column 6, lines 28 – 53.
[10] Clark, column 4, lines 11 – 20.
[11] Clark, column 5, lines 36 – 44.

- a system wherein navigational data are encrypted, and the encryption key is encrypted in turn.[12]

Therefore Claims 3 and 4 are novel and non-obvious in view of Clark.

As already discussed, Clark does not disclose nor suggest any request and authentication procedure, and the decryption key is simply broadcast in an encoded form. Instead, Clark discloses:

- the possibility of providing privileged users with the master key used for generating the encryption key, so that privileged users benefit from an unlimited access to high-precision navigational data;[13] and
- the possibility of providing privileged users with the master key used for generating the encryption key, so that privileged users benefit from an unlimited access to high-precision navigational data.[14]

Therefore Claim 5 and 7 are novel and non-obvious in view of Clark.

Clark also does not disclose nor suggest the use of a "basic" and a "supplementary" interpretation key; giving access to a different level of precision of navigational data. On the contrary, the cited passage at column 4, lines 45 - 65 makes clear that, according to Clark, users either receive the "full" decryption key or not, but there are no "basic" and "supplementary" keys. Therefore Claim 11 is novel and non-obvious in view of Clark.

Clark also does not disclose nor suggest a method wherein each transformation function participating in the definition of a decryption key is announced to the user servicing stations with an advance in time with respect to its application to the positioning signals sent out by the corresponding satellite. At column 7, line 50 to column 8, line 30, Clark simply suggests that the users acquire the decryption key even when the navigational data are not

[12] Clark, column 7, lines 1 – 14.
[13] Clark, column 6, lines 33 to 39.
[14] Clark, column 5, line 57 to column 6, line 43.

encrypted, in prevision of the possibility that the encryption mode will soon begin. Therefore Claim 12 is novel and non-obvious in view of Clark.

Claim 18 is also novel and non-obvious in view of Clark because Clark does not disclose user servicing stations which receive the decryption key from a master station and transmit it to the users on request.

As already discussed, in Clark there is no request from the users, therefore there is no request signal whose emission is automatically repeated. At column 8, lines 9 – 43, Clark discloses a system wherein a decryption key is periodically transmitted by satellite, together with positioning data. Therefore Claim 20 is novel and non-obvious in view of Clark.

Applicants have considered the Gaukel reference and submit that Gaukel does not disclose a system and method according to the present invention as claimed, and cannot suggest Applicants' invention, as Gaukel deals with a completely different problem (monitoring and tracking individual, instead as restricting access to high-precision navigational data).

As none of the cited prior art, individually or in combination, disclose or suggest all the elements of independent Claims 1 and 15, Applicants submit the inventions defined by Claims 1 and 15, and all claims depending therefrom, are not anticipated and are not rendered obvious by the asserted references for at least the reasons stated above.[15]

[15] MPEP § 2142 "...the prior art reference (or references when combined) must teach or suggest **all** the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)."

Accordingly, in view of the present amendment and in light of the previous discussion, Applicants respectfully submit that the present application is in condition for allowance and respectfully request an early and favorable action to that effect.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Michael E. Monaco
Registration No. 52,041

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

GJM/MEMO/kkn
I:\ATTY\MM\AMENDMENT\369\208536.AM DUE MARCH 16..DOC